6.7 Modular Arithmetic

In this section, we'll explore some properties of modular arithmetic that will be useful in the next chapter, when we study cryptographic algorithms based on modular arithmetic. First, recall the definition of modular equivalence from 6.1 An Introduction to Number Theory.

Definition. Let $a, b, n \in \mathbb{Z}$, and assume $n \neq 0$. We say that a **is equivalent to** b **modulo** n when $n \mid a - b$. In this case, we write $a \equiv b \pmod{n}$.[1]

[1] One warning: the notation $a \equiv b \pmod{n}$ is not exactly the same as `mod` or `%` operator you are familiar with from programming; here, both a and b could be much larger than n, or even negative.

This definition captures the idea that a and b have the *same remainder* when divided by n. You should think of this congruence relation as being analogous to numeric equality, with a relaxation. When we write $a = b$, we mean that the numeric values of a and b are literally equal. When we write $a \equiv b \pmod{n}$, we we mean that if you look at the remainders of a and b when divided by n, those remainders are literally equal.

We will next look at how addition, subtraction, and multiplication all behave in an analogous fashion under modular arithmetic. The following proof is a little tedious because it is calculation-heavy; the main benefits here are practicing reading and using a new definition, and getting comfortable with this particular notation.

Theorem. For all $a, b, c, d, n \in \mathbb{Z}$, if $n \neq 0$, if $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$, then:

1. $a + b \equiv c + d \pmod{n}$
2. $a - b \equiv c - d \pmod{n}$
3. $ab \equiv cd \pmod{n}$

Translation. We will only show how to translate and prove (2), and leave (1) and (3) as exercises.

$\forall a, b, c, d, n \in \mathbb{Z},\ \big(n \neq 0 \wedge (n \mid a - c) \wedge (n \mid b - d)\big) \Rightarrow n \mid (a - b) - (c - d)$.

Proof. Let $a, b, c, d, n \in \mathbb{Z}$. Assume that $n \neq 0$, $n \mid a - c$, and $n \mid b - d$. This means we want to prove that $n \mid (a - c) - (b - d)$.

By the Divisibility of Linear Combinations Theorem, since $n \mid (a - c)$ and $n \mid (b - d)$, it

divides their difference:

$$n \mid (a-c)-(b-d)$$
$$n \mid (a-b)-(c-d)$$

■

Modular division

The above example stated that addition, subtraction, and multiples all preserve modular equivalence—but what above division? The following statement is a "divide by k" property, but is actually **False**:[2]

[2] A good exercise is to disprove this statement!

$$\forall a, b, k, n \in \mathbb{Z},\ n > 0 \wedge ak \equiv bk \pmod{n} \Rightarrow a \equiv b \pmod{n}$$

For the real numbers, division $\frac{x}{y}$ has a single gap: when $y = 0$. As we'll see in the next theorem, division in modular arithmetic can have many such gaps, but we can also predict exactly where these gaps will occur.

Theorem. (*Modular inverse*) Let $n \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$.
If $\gcd(a, n) = 1$, then there exists $p \in \mathbb{Z}$ such that
$ap \equiv 1 \pmod{n}$.

We call this p a **modular inverse of a modulo n**.

Translation.
$\forall n \in \mathbb{Z}^+, \forall a \in \mathbb{Z},\ \gcd(a, n) = 1 \Rightarrow \left(\exists p \in \mathbb{Z},\ ap \equiv 1 \pmod{n}\right)$

Proof. Let $n \in \mathbb{Z}^+$ and $a \in Z$. Assume
$\gcd(a, n) = 1$.

Since $\gcd(a, n) = 1$, by the GCD Characterization Theorem we know that there exist integers p and q such that $pa + qn = \gcd(a, n) = 1$.

Rearranging this equation, we get that $pa - 1 = qn$, and so (by the definition of divisibility, taking $k = q$), $n \mid pa - 1$.

Then by the definition of modular equivalence, $pa \equiv 1 \pmod{n}$.

■

From this theorem about modular inverses, we can build up a form of division for modular arithmetic. To gain some intuition, first think about division $\frac{a}{b}$ as the *solution* to an equation of the form $ax = b$. We'll turn this into a statement about modular equivalence now.

Example. Let $a \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$. If $\gcd(a, n) = 1$,
then for all $b \in \mathbb{Z}$, there exists $k \in \mathbb{Z}$ such that

$ak \equiv b \pmod{n}$.

Translation. This statement is quite complex! Remember that we focus on translation to examine the structure of the statement, so that we know how to set up a proof. We aren't going to expand every single definition for the sake of expanding definitions.

$\forall n \in \mathbb{Z}^+, \forall a \in \mathbb{Z},\ \gcd(a,n) = 1 \Rightarrow \big(\forall b \in \mathbb{Z},\ \exists k \in \mathbb{Z},\ ak \equiv b \pmod{n}\big)$.

Discussion. So this is saying that under the given assumptions, b is "divisible" by a modulo n. This comes after the theorem about modular inverses, so that should be useful. The conclusion is "there exists a $k \in \mathbb{Z}$ such that…" so that I know that at some point I'll need to define a variable k in terms of a, b, and/or n, which satisfies the congruence.

I notice that the hypothesis here ($\gcd(a,n) = 1$) matches with the hypothesis from the previous theorem, so that seems to be something I can use. That gives me a $p \in \mathbb{Z}$ such that $ap \equiv 1 \pmod{n}$
…

Wait, I can multiply both sides by b, right?!

Proof. Let $a \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$. Assume $\gcd(a,n) = 1$, and let $b \in \mathbb{Z}$. We want to prove that there exists $k \in \mathbb{Z}$ such that $ak \equiv b \pmod{n}$.

First, using the previous *Modular Inverses* theorem, since we assmed $\gcd(a,n) = 1$, we know that there exists $p \in \mathbb{Z}$ such that $ap \equiv 1 \pmod{n}$.

Second, we know from (3) of our first example above that we can modular equivalence preserves multiplication, and so we know $apb \equiv b \pmod{n}$
.

Then we let $k = pb$, and we have that $ak \equiv b \pmod{n}$. ∎

These two theorems bring together elements from all of our study of proofs so far. We have both types of quantifiers, mixed with a larger implication. We used the GCD Characterization Theorem for a key step in our proof. This illustrates the power of

separating ideas into different statements and using each one to prove the next, just like we separate code into different functions in our programs!

Exponentiation and order

The last ingredient we'll need to understand for our study of cryptography next week is the patterns that emerge when it comes to exponentiation in modular arithmetic. In normal arithmetic, powers of positive integers increase without bound, but in modular arithmetic we can focus on the *remainders* of powers, and discover some wonderful properties. For example, 10^{13} is a very large number indeed, but $10^{13} \equiv 3 \pmod 7$! In fact, because there are only a finite number of remainders for any given $n \in \mathbb{Z}^+$, for any $a \in \mathbb{Z}$ the infinite sequence of *remainders* of a^0, a^1, a^2, a^3, ... must repeat at some point.

For example, let's see what happens for each of the possible bases modulo 7:[3]

[3] Because exponentiation by positive integers corresponds to repeated multiplication, which behaves "nicely" with modular arithmetic, the list below covers all possible integers. For example, because $10 \equiv 3 \pmod 7$, we also know that $10^{13} \equiv 3^{13} \pmod 7$.

- 0: $0^1 \equiv 0 \pmod 7$, $0^2 \equiv 0 \pmod 7$
- 1: $1^1 \equiv 1 \pmod 7$, $1^2 \equiv 1 \pmod 7$
- 2: $2^1 \equiv 2 \pmod 7$, $2^2 \equiv 4 \pmod 7$, $2^3 \equiv 1 \pmod 7$, $2^4 \equiv 2 \pmod 7$
- 3: $3^1 \equiv 3 \pmod 7$, $3^2 \equiv 2 \pmod 7$, $3^3 \equiv 6 \pmod 7$, $3^4 \equiv 4 \pmod 7$, $3^5 \equiv 5 \pmod 7$, $3^6 \equiv 1 \pmod 7$, $3^7 \equiv 3 \pmod 7$
- 4: $4^1 \equiv 4 \pmod 7$, $4^2 \equiv 2 \pmod 7$, $4^3 \equiv 1 \pmod 7$, $4^4 \equiv 4 \pmod 7$
- 5: $5^1 \equiv 5 \pmod 7$, $5^2 \equiv 4 \pmod 7$, $5^3 \equiv 6 \pmod 7$, $5^4 \equiv 2 \pmod 7$, $5^5 \equiv 3 \pmod 7$, $5^6 \equiv 1 \pmod 7$, $5^7 \equiv 5 \pmod 7$
- 6: $6^1 \equiv 6 \pmod 7$, $6^2 \equiv 1 \pmod 7$, $6^3 \equiv 6 \pmod 7$

No matter which base we start with, we enter a cycle. For example, the cycle starting with 2 is $[2, 4, 1, 2, \ldots]$. We say this cycle has length 3, since it takes three elements in the sequence for the 2 to repeat. Here are the cycle lengths for each possible $a \in \{0, 1, \ldots, 6\}$:

a	**Cycle length**
0	1
1	1
2	3
3	6
4	3
5	6
6	2

For each base other than 0, there is another way of looking at the cycle length: the cycle length for base a is the smallest positive integer k such that $a^k \equiv 1 \pmod 7$. For example, $2^3 \equiv 1 \pmod 7$, and the cycle repeats at $2^4 \equiv 2^3 \cdot 2 \equiv 2 \pmod 7$.

This "cycle length" is a fundamental property of modular exponentiation, and warrants its own definition.

Definition. Let $a \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$. We define the **order of a modulo n** to be the smallest positive integer k such that $a^k \equiv 1 \pmod{n}$, when such a number exists.

We denote the order of a modulo n as $\text{ord}_n(a)$.

Something you might notice from our above table is that the cycle length for the remainders modulo 7 always divides 6. Here is another table, this time for modulo 17.

a	**Cycle length**
0	1
1	1
2	8
3	16
4	4
5	16
6	16
7	16
8	8
9	8
10	16
11	16
12	16
13	4
14	16
15	8
16	2

A similar pattern emerges: the cycle length for these bases always divides 16, which is one less than 17. And again, for each base a other than 0, the cycle length corresponding to a is the least positive integer k such that $a^k \equiv 1 \pmod{17}$.

Here is one more interesting fact about cycle length: because it is a number k such that $a^k \equiv 1 \pmod{17}$, *any* multiple n of k also satisfies $a^n \equiv 1 \pmod{17}$. For example, $13^4 \equiv 1 \pmod{17}$, and so $13^{40} \equiv (13^4)^{10} \equiv 1^{10} \equiv 1 \pmod{17}$.

Combining these two observations allows us to conclude that, at least for 17, *every* base a other than 0 satisfies $a^{16} \pmod{17}$. It is a remarkable fact that this turns out to generalize to every prime number. Proving this theorem is beyond the scope of this course, but we'll state it formally here to let you marvel at it for a moment.

Theorem. (*Fermat's Little Theorem*) Let $p, a \in \mathbb{Z}$ and assume p is prime and that $p \nmid a$. Then $a^{p-1} \equiv 1 \pmod{p}$.

Euler's Theorem

Fermat's Little Theorem is quite beautiful in its own right, but is limited in scope to prime numbers. It turns out that the key to generalizing this theorem lies with our very last definition in this chapter.

Definition. We define the function $\varphi : \mathbb{Z}^+ \to \mathbb{N}$, called the **Euler totient function** (or **Euler phi function**), as follows:

$$\varphi(n) = \left|\left\{a \mid a \in \{1, \ldots, n-1\}, \text{ and } \gcd(a, n) = 1\right\}\right|.$$

Here are some examples of the Euler totient function:

- $\varphi(5) = 4$, since $\{1, 2, 3, 4\}$ are all coprime to 5.
- $\varphi(6) = 2$, since only $\{1, 5\}$ are coprime to 6.
- In general, for any prime number p, $\varphi(p) = p - 1$, since all the numbers $\{1, 2, \ldots, p-1\}$ are coprime to p.[4]

  [4] Exercise: prove this using the definition of prime!

- $\varphi(15) = 8$, since the numbers $\{1, 2, 4, 7, 8, 11, 13, 14\}$ are all coprime to 15. Note that the ``removed'' numbers are all multiples of 3 or 5, the prime factors of 15.
- In general, for any two distinct primes p and q, $\varphi(pq) = (p-1)(q-1)$, although this is certainly not obvious, and requires a proof!

With the Euler totient function in hand, we can now state the generalization of Fermat's Little Theorem, which is something we'll use in the next chapter.

Theorem. (*Euler's Theorem*). For all $a \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$, if $\gcd(a, n) = 1$ then $a^{\varphi(n)} \equiv 1 \pmod{n}$.